

főoldal blogok fórumok szavazások HupWiki	
	Címlap
Egy hónapja ismert a Kaminsky-DNS probléma - hol tart a hazai védekezés?	
(troy 2008. augusztus 8., péntek - 13:23) Titkosítás, biztonság	
<p>A BME Híradástechnikai Tanszék CrySys Laboratóriuma a Kaminsky-féle DNS cache poisoning sebezhetőség aprójából megvizsgálta, hogy mennyire maradtak sérülékenyek a hazai DNS szerverek.</p>	
<p>Idézet:</p> <p>Sokakat érint és sokakat érdekel, hogyan halad a Kaminsky-féle DNS támadás elleni védekezés implementálása hazánkban. A hiba létezése 2008. július 8. óta ismert, és azóta elérhetőek azok a friss szoftververziók is, amelyek védelmet nyújtanak a hiba ellen. Vizsgálatunk során leellenőriztük, hogy a hazai DNS szerverek gazdái telepítették-e a védekezéshez ma elengedhetetlen szoftvereket. Az eredmények azt mutatják, hogy a szerverek mintegy kétharmada jelenleg nem védett a támadás ellen. A nagy szolgáltatók többsége már implementálta a javasolt védelmet, de ez még nem elég az ügyfelek védelmére.</p>	
<p>Idézet:</p> <p>A Dan Kaminsky nevével jegyzett internetes DNS támadás lehetőségéről a nagyközönség 2008. július 8-án szerzett tudomást, amikor számos gyártó, fejlesztő előre egyeztetett módon egyszerre jelentett be egy korábban ismeretlen hiba ellen védekezést nyújtó javítócsomagot. A hiba súlyossága miatt egyedülálló összefogás született, és ennek eredménye volt az, hogy a hiba kijavítása napvilágra került, de a hiba nem. Az eredeti tervek szerint Dan Kaminsky 2008. augusztus 7-én ismerteti a hiba és a támadás pontos módszerét a Black Hat 2008 konferencia keretében. Így 30 napja volt a rendszergazdáknak és üzemeltetőknek, hogy a rendelkezésre álló javításokat teszteljék és telepítsék. Fontos megjegyezni ezen a ponton, hogy ipari környezetben egy szoftver frissítése, még ilyen súlyos esetben sem egy egyszerű feladat. A magas rendelkezésre állás garantálása érdekében a szoftvereket tesztelni kell, a cég-specifikus szoftvermódosításokat pedig átdolgozni az újabb, javított változatba. Az otthoni felhasználóknak és kis cégeknek pár nap is elég lehetne a szoftverek frissítésére, de a teljes Internet frissítése időigényes feladat. Az eredeti terveket, a 30 napos „haladékot” módosította az, hogy az idők során kb. 2 héttel a javítások bejelentése után az Interneten körvonalazódott a biztonsági probléma mibenléte, és most, a hiba publikálásának időpontjában, kis részletek kivételével már mindenki tudja, mi is a hiba és rendelkezésre állnak a támadásokra készített programok is. Letelt tehát a 30 nap, ami alatt mindenki frissíthette szoftvereit, hogy azok védettek legyenek. Sokakban felmerül a kérdés, hogy Magyarországon mennyire készültünk fel ezalatt a súlyos probléma kezelésére és nyugodtan tölthetjük-e be kedvenc bankunk elektronikus banki felületét az Interneten keresztül. Ezt vizsgáltuk meg Műegyetem Híradástechnikai Tanszékének CrySys Laboratóriumában (www.crysys.hu) 2008. augusztus 6-án.</p>	
<p>Vizsgálatunk tárgyai a hazai DNS kiszolgálók voltak. Azt kívántuk felderíteni, hogy a Magyarországon üzemelő DNS kiszolgálók milyen arányban sebezhetiek a támadás szempontjából, és mennyi a biztonságos szerver. Fontos azonban tudni, hogy egy ilyen vizsgálat komplikált és nem mindig nyújt egyértelmű eredményt, mert nincsen olyan adatbázis, ahonnan kiolvasható lenne az összes szerver címe, vagy ismerhető lenne az összes hálózat egyedi beállítása. Vizsgálatunk tehát nem feltétlenül reprezentatív, de a hozzáférőknek fontos információkkal szolgál a hazai biztonsági kultúra helyzetéről.</p>	
<p>A felmérés teljes eredménye megtalálható ebben a tanulmányban.</p> <p>» A hozzászóláshoz belépés szükséges 2475 olvasás</p>	
Hozzászólás megjelenítési lehetőségek	
Beágyazott (teljes) <input type="checkbox"/> Dátum - régebbiek elől <input type="checkbox"/>	
300 egy oldalon <input type="checkbox"/> <input type="button" value="Beállítás"/>	
<p>A választott hozzászólás megjelenítési mód a „Beállítás” gombbal rögzíthető.</p>	
(algernon 2008. augusztus 8., péntek - 14:11)	
<p>A "vedettség" sem er tulzottan sokat onmagaban: http://tservice.net.ru/~s0mbre/blog//devel/networking/dns/2008_08_08</p>	
A hozzászóláshoz belépés szükséges permalink	
(yeo 2008. augusztus 8., péntek - 14:38)	
<p>nemis értem azokat akik vállat vonogatnak ezzel kapcsán, igenis elég komoly probléma ez...</p>	
A hozzászóláshoz belépés szükséges permalink	

Is -1

- /boot
- /blogok
- /faq
- /fórumok
- /fórum friss
- /ftp
- /hír küldése
- /huplite
- /keresés
- /képek
- /regisztráció
- /szavazások
- /videók
- /visszajelzés
- /kerestetik
- /statisztika
- /szerver
- /támogatók

Történelem

UNIX:

- 1941 - 1979
- 1980 - 1999
- 2000 - napjainkig


BSD:

- BSD I. rész
- BSD II. rész
- BSD III. rész
- BSD IV. rész

Népszerű témák

Apple [Bejelentés](#)
Bug [Debian](#) [Egyéb](#)
[FreeBSD](#) [Hír](#)
Hardver [Internet](#)
Játék [Kernel](#)
[Linux](#) [Microsoft](#),
[Windows](#) [Mozilla](#)
[NetBSD](#)
[OpenBSD](#) [Open](#)
[Source](#) [openSUSE](#) [Red](#)
[Hat](#), [Fedora](#) [SUN](#)
[Microsystems](#)
Szerszám [Szoftver](#)
[Titkosítás](#), [biztonság](#)
[Ubuntu](#) [Linux](#) [X](#)
[Window](#) tovább

Ajánlott böngésző



Take back the web

IRC

A HUP hivatalos IRC csatornája, a [#hup.hu](#)

Keresés

web hup.hu

Navigáció

- friss tartalom
- hírolvasó

Google Hirdetések

[Free Dynamic DNS Service](#)
No-IP Dynamic DNS. Free Trial! Domain Monitoring & Registration.
www.No-IP.com

[POP3 levelező szerver](#)
Bármilyen Windowson működő levelező szerver. Ingyenes próbaverzió!
www.vpop3.hu

Belépés

Felhasználói név: *

Jelszó: *

Elfelejtett jelszó

(x)

- [Masterfield: INTEGRATE képzsékek - pénz visszafizetési garanciával](#)

HupWiki

- [Linux BSD Solaris összehasonlítás](#)
- [BSDanywhere](#)

tovább

Friss blogbejegyzések

- "Új" broadcom meghajtó? vége a rémálomnak?
- Ventrilo szoba
- Peking Express #3
- Holnap előadás, gyertek...
- Mosolygenerátor - No comment
- Peking Express #2
- Láthatatlan kéz
- Numerikus billentyűzet Putty alatt
- hoax, ami nem hoax
- Hibás ablakfejléc

tovább

HUP napi hírlévíl

megtalálható a

Freenode
(irc.freenode.net)

hálózaton. Nézz be!

Hardver



(algernon | 2008. augusztus 8., péntek - 15:57)

Valóban az. En azokat nem értem akik felrakják a port-randomizalo patcheket es azt hiszik biztonságban vannak, es vedettek. Pedig közel sem.

A hozzászóláshoz belépés szükséges [permalink](#)

(bra | 2008. augusztus 8., péntek - 19:53)

Elég sok védelmi lehetőség van:

- random query ID-k
- random forrás portok
- random forrás IP-k
- nagy cache-ek (vagy épp ellenkezőleg: a cache kikapcsolása :)
- a válaszok körütekintő értelmezése ("trójai" rekordok, kis-nagybetű váltás, ellenőrzés, stb)
- a nem érvényes válaszokat küldő források rate limitálása, egyre hosszabb tiltása (fail close, DoS :)
- az autoritativ szerverek "megválogatása" (random, leggyorsabb)
- spoofing tiltása az access hálózatodban, a bejövő vonalakon forrásellenőrzés (sokszor nehéz a routing policyk és egyéb tényezők miatt)
- rekurzió korlátozása csak a saját klienseidre (akiknek a címeit kívülről nem fogadod el, lásd előző)
- TCP, DNSSEC :)

Meg még biztos jópár dolog, amihez gondolkozni is kellene (de éjszakázás után az most nem megy). :)

Persze nem mindenkinek van lehetősége ezt mind (és a többit) meglépni...

A hozzászóláshoz belépés szükséges [permalink](#)

(yeo | 2008. augusztus 9., szombat - 3:38)

ezek közül a védelmek közül majdnem mind megkerülhető/kijátható, a megoldás a DNSSEC lenne, de ügytűnik jóideig erre még várni kell.

A hozzászóláshoz belépés szükséges [permalink](#)

(bra | 2008. augusztus 9., szombat - 16:56)

Úgy tűnik az oktatás színvonalának újbóli emelkedésére is. :(

Aki kicsit is érti a dolgot, tisztában van vele, hogy a DNS jelen formájában nem kijáthatatlan. De vannak lépések, amelyekkel megnehezíthető a folyamat, ezekről írtam (ami nekem éppen eszembe jutott).

A DNSSEC (és a TCP, ha már itt tartunk) olyan dolgok, amelyek alapvetően nem a kérdezőn múlnak.

Azon sem csodálkoznék, ha nagy hirtelen mindenki elkezdéné használni a DNSSEC-et, és a következő hasonló konferencián annak (általános, vagy egy nagyobb telepítéssel rendelkező konkrét implementációjának) hibájáról hallhatnánk...

A címhamisítás pedig olyan dolog, hogy ha minden ISP rendesen védekezne, sokkal, de sokkal nehezebb lenne ilyen támadásokat kivitelezni.

A hozzászóláshoz belépés szükséges [permalink](#)

(yeo | 2008. augusztus 9., szombat - 23:18)

nem igazán értem eztafajta reagálást, az oktatás egyáltalán hogy jön képbe ?

a "minden ISP rendesen védekezne", egyetértünk ebben hogy ez utópia, pont ebből kifolyólag arról próbáltam lerántania leplet, hogy hiába vonogatnak egyesek vállat hogy nem érdekes eza sebezhetőség, igenis érdekes, ésamellet hogy a lehető legszorosabban kéne védekezni ellene, lassan az utódot is elkéne kezdeni felnevelgetni.

A hozzászóláshoz belépés szükséges [permalink](#)

(mogorva | 2008. augusztus 8., péntek - 15:30)

Volt valahol egy URL, amivel lehetett csekkolni a DNS-eket. Megvan vkinek?

A hozzászóláshoz belépés szükséges [permalink](#)

(spymorass | 2008. augusztus 8., péntek - 15:33)

<http://www.doxpara.com/?p=1162>

A hozzászóláshoz belépés szükséges [permalink](#)

(mogorva | 2008. augusztus 10., vasárnap - 18:44)

kösz!

A hozzászóláshoz belépés szükséges [permalink](#)

(Dolphy | 2008. augusztus 8., péntek - 16:59)

Van valakinek valami jó anyaga arról, hogy hogyan is működik részletesen ez a támadás? A legjobb lenne magyarul, esetleg egy könnyebben érthető angol.

A hozzászóláshoz belépés szükséges [permalink](#)

(Husky | 2008. augusztus 8., péntek - 17:49)

Email cím:

Feliratkozás

3737 readers
BY FEEDBURNER

__define__ kernel

- 2.6.28-rc2-mm1: stable mm patch
- 2.6.28-rc2-git3: stable snapshot
- 2.6.28-rc2: stable prepatch
- 2.6.27.4: stable
- 2.4.36.8: 2.4 release

[tovább](#)

Legfrissebb HUP képek

- MaXX Desktop DR2 Xinerama
- Linux háttérkép kezdőknek
- iTunes 8.0.1 Ubuntu-n VMware Unity-vel
- Pandora - linuxos játékkonzol
- Pandora - linuxos játékkonzol

[tovább](#)

Szavazás

Kerüljenek-e kiszűrésre a HUP fórum center blokkból a ! szakmai topikok?

Igen.

55%

Nem.

45%

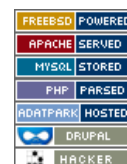
Összes szavazat:
690

52 hozzászólás
3323 olvasás
korábbi szavazások

Új felhasználók

- andriscom
- therieper47
- erdeszimi
- ricky1
- secretx

Információ



Tartalom megosztás



Megkered a kiszemelt DNS-t, hogy oldjon fel neked egy nevet. Majd azonnal kuldod is ra azt a választ amit te szeretnél kapni (a trukk az, hogy nem muszaj hostnevet választanod, mehet kamu redirect is). Ez jó eséllyel előbb fog hozzá megerkezni mint a valódi válasz a valódi DNS-tól, és neked hiszi majd el -> azt irsz bele amit akarsz.

Ezt nehezíti a TXID, viszont az csak 16 bites. Ezt nehezíti a random port, viszont vannak már gigabites kártyák. Ezt nehezíti ha nem all veled szóba a DNS, viszont általában van mogotte mailszerver/IDS, aki igen. Ezt nehezíti a TTL, de... ez mind le van írva Kaminsky prezentaciojában. :)

[A hozzászóláshoz belépés szükséges](#) [permalink](#)

(boldi | 2008. augusztus 8., péntek - 22:58)

Amit Husky ír az kb. a korábbi tudás. Csak akkor volt esélyed, ha eltaláltad a 16 bites TXID-t. Ha nem találtad el, ki kellett várni a TTL-t (ez egy előbbi kommenthez is fontos adalék) és akkor tudtad újra támadni a célpontot. Mondjuk két nap múlva. És persze egyszerre elküldhetsz jó sok TTL-t, van esélyed, hogy a másik szerver előtt többszáz a tiedből fut be. De nem 64k. A csavar az, hogy a szervertől lekérdezed az

1.dc.hu
2.dc.hu
3.dc.hu

..

sok.dc.hu címekeket. Mindig elküldesz egy sereg különböző TXID-vel válaszokat, mondjuk 200-at. Egyszer, valamikor te fogsz győzni, és a te válaszod lesz a friss az adott

33643.dc.hu kérésre.

Nos, ekkor jön a csel. Oké, hogy sikerült átírnod a célgépen a 33643-at, de az nem volt célod, ki a francnak okoz örömet. Viszont küldhetsz egy olyan választ is, hogy (33643.dc.hu -> nem én vagyok a felelős, keresd fel ezért a www.dc.hu -t, ja és megsúgom, a www.dc.hu IP címe 6.6.6.6.) Ez a zárójeles rész maga a teljes válasz, mindenestül.

Nos, ekkor a célzott szerver nemcsak a 33643-at, hanem a www.dc.hu -t is megtanulja rosszul, ha még nem ismerte addig. És így sokkal hatékonyabb támadás született, mint akkor, amikor Husky módszerével csak "egyetlen címet" támadtak. (mert most sokon keresztül támadható az egy)

[A hozzászóláshoz belépés szükséges](#) [permalink](#)

(Husky | 2008. augusztus 9., szombat - 1:55)

(Lásd zárójeles rész az eredeti hozzászólásomban, és a hozzászólásom végén látható három pont a TTL után ;))

De végülis jogos, magyar leírást kerestem, nem kellett volna ajánlanom az eredeti doksit. :)

[A hozzászóláshoz belépés szükséges](#) [permalink](#)

(algernon | 2008. augusztus 9., szombat - 2:28)

Mint eredeti hozzászólásomban említettem, a "vedettség" (ami a legtöbb embernek, aki nem olvas utána, kb a port randomizációt jelenti) nem ér sokat onmagában. Ez az utolsó szó a kulcs. ;)

Egyeb finomságokkal kiegészítve már el lehet venni előbb-utóbb a kedves próbalkozók kedvet, és elhetünk tovább boldogan. De ha csak annyit teszünk, hogy felrakjuk a legújabb bindet és reménykedünk, annyi erővel akár tojhatnánk is az egész temára.

Talalkoztam jónéhány olyan emberrel, aki így tett, felrakta, megnezte jajdejo, random portok, és utána az úgy le van zárva.

Edit: bra postjara akart menni, csak nem tudok kattintani így hajnali fel háromkor.

[A hozzászóláshoz belépés szükséges](#) [permalink](#)

(botika | 2008. augusztus 9., szombat - 22:30)

Asszem szorakozik velem valaki... Illetve az intranetes Active Directory nevszervereivel. Milyen lehetosegem lehet megfogni az illetot?

[A hozzászóláshoz belépés szükséges](#) [permalink](#)

Olcsó szerver elhelyezés

Két évre fix áron: 9900Ft/hónap+áfa

Szerverhosting BIX kapcsolattal.

BestServers.eu Hosting

Google Hirdetések

Logo and hup.hu content copyright © 2000-2008 by Gabor Micsko
All trademarks and copyrights on this page are owned by their respective owners.